Amendments to the Claims:

1. (Currently Amended) A ~~secured communication~~ method implemented by a server system to secure communications between a service provider and a mobile device in ~~for~~ a mobile communications network, the method comprising:

receiving a request from the mobile device to provide a unique security key ~~to a mobile device connected to the mobile communications network~~;

generating a unique security key ~~for the requesting mobile device~~, in response to receiving the request from the mobile device~~receiving a unique identification number from the mobile device~~;

storing the unique security key in association with an identifier of the mobile device in a first data storage mechanism in the server system~~in association with the unique identification number identifying the mobile device, wherein the first data storage mechanism is accessible to a server system connected to the mobile device over a wide area communicatoin network, and wherein the first data storage mechanism is not directly accessible by the mobile device~~;

providing the unique security key to the mobile device, wherein the mobile device stores the unique security key in a second data storage mechanism in the mobile device;

receiving a request from the service provider to provide the unique security key, wherein the service provider requests the unique security key in order to establish a secure communication session with the mobile device ~~for the mobile device to a service provider such that the service provider can provide a service to the mobile device based on the unique security key~~; and

providing the unique security key to the service provider, in response to determining that the service provider is included in a list of approved service providers, wherein the list of approved service providers is updatable by the mobile device, and wherein the secure communication session is established between the service provider and the mobile device, in response to the service provider presenting the unique security key to the mobile device for authentication.~~approving the request to provide the unique~~

~~security key to the service provider based on content of a list of service providers stored in a second data storage mechanism,~~

~~wherein the second data storage mechanism is directly accessible by the mobile device,~~

~~wherein the content of the list of service providers is editable by a user of the mobile device by way of directly accessing the second data storage mechanism via the mobile device.~~

2. (Currently Amended) The method of claim 1, wherein the list of approved service providers is stored in at least one of the first and second data storage mechanisms~~further comprising:~~

~~denying the request to provide the unique security key, if the service provider is not approved to receive the unique security key for the mobile device according to the content of the list of service providers stored in the second data storage mechanism~~.

3. (Canceled)

4. (Previously Presented) The method of claim 1, wherein the second data storage mechanism is a memory chip embedded in the mobile device.

5. (Previously Presented) The method of claim 1, wherein the second data storage mechanism is an identity module removably insertable in the mobile device.

6. (Previously Presented) The method of claim 1, wherein the second data storage mechanism is a SIM card for the mobile device.

7. (Canceled)

8. (Currently Amended) The method of claim 1, wherein the ~~unique identification number~~identifier is at least one of the mobile device's electronic serial number (ESN), international mobile equipment identity (IMEI) or a phone number.

9-15 (Canceled)

16. (Currently Amended) A system configured to secure communications between a service provider and a mobile device in a mobile communications network, the system comprising:

a receiver configured to:

receive a request from the mobile device to provide a unique security key; and

receive a request from the service provider to provide the unique security key, wherein the service provider requests the unique security key in order to establish a secure communication session with the mobile device;

a processor configured to:

generate a unique security key, in response to receiving the request from the mobile device; and

store the unique security key in association with an identifier of the mobile device in a first data storage mechanism in the server system;

a transmitter configured to:

provide the unique security key to the mobile device, wherein the mobile device stores the unique security key in a second data storage mechanism in the mobile device; and

provide the unique security key to the service provider, in response to determining that the service provider is included in a list of approved service providers, wherein the list of approved service providers is updatable by the mobile device, and wherein the secure communication session is established between the service provider and the mobile device, in response to the service provider presenting the unique security key to the mobile device for authentication.

~~A secured communication system for a mobile communications network, the system comprising:~~

~~a logic unit for receiving a request to provide a security key to a mobile device connected to the mobile communications network;~~

~~a logic unit for generating a unique security key for the requesting mobile device in response to receiving a unique identification number from the mobile device;~~

~~a logic unit storing the unique security key in a first data storage mechanism in association with the unique identification number identifying the mobile device,~~

~~wherein the first data storage mechanism is accessible to a server system connected to the mobile device over a wide area communicatoin network and wherein the first data storage mechanism is not directly accessible by the mobile device;~~

~~a logic unit for receiving a request to provide the unique security key for the mobile device to a service provider such that the service provider can provide a service to the mobile device based on the unique security key; and~~

~~a logic unit for approving the request to provide the unique security key to the service provider based on content of a list of service providers stored in a second data storage mechanism,~~

~~wherein the second data storage mechanism is directly accessible by the mobile device,~~

~~wherein the content of the list of service providers is editable by a user of the mobile device by way of directly accessing the second data storage mechanism via the mobile device.~~

17. (Currently Amended) The system of claim 16, wherein the list of approved service providers is stored in at least one of the first and second data storage mechanisms~~further comprising:~~

~~denying the request to provide the unique security key, if the service provider is not approved to receive the unique security key for the mobile device according to the content of the list of service providers stored in the second data storage mechanism~~.

18. (Previously Presented) The system of claim 16, wherein the second data storage mechanism is a memory chip embedded in the mobile device.

19. (Previously Presented) The system of claim 16, wherein the second data storage mechanism is an identity module removably insertable in the mobile device.

20. (Previously Presented) The system of claim 16, wherein the second data storage mechanism is a SIM card for the mobile device.

21. (New) The system of claim 16, wherein the identifier is at least one of the mobile device's electronic serial number (ESN), international mobile equipment identity (IMEI), or phone number.